U.S. Export Controls Quick Reference Sheet for Partners and Sales

As part of Fortinet's on-going global trade compliance communications, this document may be used as a quick reference sheet for use by Fortinet Partners and Sales. This document serves as a friendly reminder of the US export control regulations and how they affect your sales efforts, and focuses on 5 rudimentary concepts, some of which are based on broad regulatory requirements, and others specific to sales of strong encryption product:

1. Which countries Fortinet does NOT sell to. (Note: Our Partners by contract and regulation must also comply with U.S. embargo and sanction and export/import control regulations and those of the countries they operate in.)

2. Which countries are "sensitive" and thus require additional due diligence review or export licensing in order to legally sell to such countries. Please contact your trade compliance personnel or Fortinet Global Trade Compliance at exportalert@fortinet.com as soon as you have a possible **new** business prospects in these countries, or existing business where end-user/end-use requires licensing review.

3. Which Government End Users require an export license before Fortinet Partners can sell to them. Contact your trade compliance personnel or Fortinet Global Trade Compliance at exportalert@fortinet.com, as soon as you have a possible business prospects with such government end users.

4. Which End-User activities are subject to "proliferation controls", and require an export license before Partners can sell to parties involved in these activities.

5. Check parties against the U.S. Restricted Parties lists – These may be accessed by paid subscription services or by visiting the U.S. Bureau of Industry & Security website at: http://www.bis.doc.gov/complianceandenforcement/liststocheck.htm

I. Fortinet and our partners are prohibited from selling/providing services to the following Embargoed/Sanctioned/Terrorist supporting countries which are currently:

1. Cuba
2. Iran
3. North Korea
4. Sudan
5. Syria
6. The Crimea Region of Ukraine

II. "Sensitive" countries- (also referred to as Country D: Supplement no. 1 to Part 740 of the EAR) - Contact your trade compliance personnel ASAP regarding business prospects to review regulatory requirements and avoid unnecessary delays:

Afghanistan, Armenia, Azerbaijan, Bahrain, Belarus, Burma, Cambodia, Central African Republic, China, Democratic Republic of Congo, Cote D'Ivoire, Cyprus, Egypt, Eritrea, Georgia, Haiti, Iraq, Israel, Jordan, Kazakhstan, Kuwait, Kyrgyzstan, Laos, Lebanon, Liberia, Libya, Macau, Moldova, Mongolia, Oman, Pakistan, Qatar, Russia, Saudi Arabia, Somalia, Sri Lanka, Taiwan, Tajikistan, Turkmenistan, Ukraine, United Arab Emirates, Uzbekistan, Venezuela, Vietnam, Yemen, Zimbabwe.

You'll note that this list contains some countries wherein you may currently do business. Categorization as "sensitive" doesn't mean that you cannot or do not sell to these countries. There may be additional licensing requirements depending on who the end-user or what the end-use is in these countries. That's why we highly encourage you to contact your trade compliance personnel or Fortinet's Global Trade Compliance Department as soon as you are exploring a new business prospect to address export regulatory issues early in the deal cycle.

III. Government end-users – Purchase of Fortinet's strong encryption products by government end-users outside of the ENC favorable treatment countries (formerly called the EU "license free zone") require an export license. An End-user Certification Letter of EUCL is a supporting document required for all licensable shipments from Fortinet https://fpp.fortinet.com/forticrm/EUCL/New.do?type=standard&lang=en

The list of ENC Favorable Treatment Countries are:
Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, and United Kingdom.

- **A government end-user (as applied to encryption items) is any foreign (Non-U.S.) central, regional, or local government department, agency or other entity performing governmental functions; including governmental research institutions, governmental corporations or their separate business units…**

Partners must obtain an export license for strong encryption products when moving stock inventory to a government end-user. Units that do not ship against an export license are blocked and will not receive updates and/or may not be registered.

IV. Proliferation Controls - Avoid unnecessary delays, and contact your trade compliance personnel ASAP regarding all prospective orders destined for End-Users involved in designing, developing, producing, stockpiling or supporting activities in:
1. Chemical or biological weapons
2. Nuclear weapons or Power plants
3. Missiles
4. Defense/Military

An export license is required before you can legally sell to entities involved in these lines of business. In many cases there is a presumption of denial for export licensing in these categories.

V. U.S and foreign restricted parties lists – You must always check all parties to your transaction against both the U.S. Restricted Parties lists, and those in the countries in which you operate.

These may be accessed by paid subscription services which we highly encourage you subscribe to, which include both U.S. and non-U.S. lists. You may also visit the U.S. Bureau of Industry & Security website at: http://www.bis.doc.gov/complianceandenforcement/liststocheck.htm to check U.S. Restricted Parties lists.

Why is this important?

- **There are stiff civil and criminal penalties for U.S. and foreign parties violating U.S. export laws.**
- **Criminal penalties can reach 20 years imprisonment and $1 million per violation. Administrative monetary penalties can reach $11,000 per violation, and $120,000 per violation in cases involving items controlled for national security reasons.**
- **Civil penalties can include significant fines and/or loss of export privileges.**
- **Collateral effects of violations can result in adverse publicity, exclusion from participation in U.S. Government contracts, and restrictions on export/importing into and out of the United States.**
- **Violations of laws, regulations, rules and orders may subject the violator (you) to individual criminal or civil liability.**

Remember, you are responsible for exporting/importing Fortinet products in accordance with the requirements of the U.S. Export Administration Regulations, and applicable local/foreign export/import regulations. Factors, such as the specific product, end-user, end-use and country of ultimate destination, may affect the export licensing requirements. You are urged to consult the U.S. Export Administration Regulations, the Bureau of Industry & Security's Export Counseling Division, Customs, and other appropriate resources such as an attorney or consultant specializing in trade compliance before exporting/importing Fortinet's products.

Please direct any inquiries to exportalert@fortinet.com.